CLAIMS

What is claimed is:

1. A method of monitoring access to a protected database resource comprising:

identifying an attempt to access the database resource, the access attempt being local and directed to an access gateway of the database resource;

intercepting the identified attempt to access the database resource, intercepting occurring in a prioritized manner with respect to receipt of the access attempt by the access gateway; and

transmitting, in a nondestructive manner, the intercepted access attempt to a local agent, the nondestructive manner operable to preserve the intercepted access attempt for successive receipt by the access gateway.

2. The method of claim 1 wherein the access attempt is deterministic of a DB instruction, and the local agent is in communication with a data security device operable to analyze the propriety of the access attempt from objects and data values referenced by the DB instruction.

3. The method of claim 1 wherein intercepting in a prioritized manner further comprises:

receiving the access attempt into an interception register prior to receipt by the access gateway;

invoking a prioritized request to activate a reading operation of the interception register, invoking occurring prior to activation of a read operation of the access attempt on behalf of the access gateway; and

reading the access attempt from the interception register, the interception register subsequently appearing undisturbed to the access gateway.

4. The method of claim 1 further comprising, prior to identifying the access attempt, establishing an IPC intercept operable to receive IPC communications directed to the access gateway prior to receipt of the IPC communication by the access gateway.

5. The method of claim 1 wherein identifying the access attempt further comprises listening, at a common access point, for an incoming connection to the database resource, the common access point adapted to aggregate access attempts to the database resource from a plurality of access mediums.

6. The method of claim 2 wherein transmitting further comprises rerouting the intercepted access attempts to the data security device, the data security device operable to offload data security decisions as a consolidated appliance, the offloaded data security decisions relieving the host from processing the data security decisions.

7. The method of claim 1 wherein the local agent performs rerouting of local access attempts in a lightweight manner such that the data security device is operable to receive local and remote access attempts, wherein security coverage of the DB server for network and local access attempts occur via a common appliance.

8. The method of claim 1 wherein intercepting further comprises:

receiving, from a notification object responsive to an event handler, an indication of an IPC communication indicative of a DB access attempt;

identifying an instruction register in a shared memory area, the instruction register having a database instruction corresponding to the access attempt;

retrieving the DB instruction from the identified instruction register; and

transmitting the retrieved DB instruction to the data security device.

9. The method of claim 1 wherein the intercepting further comprises:

determining an IPC mechanism to be employed by a local client for accessing the DB resource;

establishing an IPC intercept from a common access point employed by database clients for accessing the DB resource; and

receiving the access attempt at the local agent via the IPC intercept prior to receipt of the access attempt by the access gateway.

10. The method of claim 9 wherein determining the IPC mechanism further comprises:

identifying a plurality of access paths to a protected resource;

identifying a common access point for the access paths to the protected resource, access attempts occurring exclusively via the identified access point for the identified access paths.

11. The method of claim 1 further comprising:

establishing an interface wrapper between the access gateway and the local client, the interface wrapper operable to identify an IPC mechanism adapted to transport communications between the access gateway and the local client; and

modifying the identified IPC mechanism to inform the local agent of the communications between the access gateway and the local client prior to informing the access gateway of the communication.

12. The method of claim 11 wherein the IPC mechanism is a shared memory portion including a plurality of instruction registers, the instruction registers operable to buffer a DB instruction for receipt by the access gateway.

13. The method of claim 1 wherein the local agent is a lightweight agent operable to intercept the access attempt and transmit the intercepted DB instruction to a data security device, the local agent having a substantially insignificant effect on a DB host supporting the DB server.

14. The method of claim 1 wherein intercepting further comprises

blocking the intercepted access attempt from receipt by the access gateway, and selectively unblocking the access attempt depending on a data security decision.

15. The method of claim 14 further comprising:

computing the data security decision at the data security device; and

transmitting the data security decision to the local agent, the local agent operable to permit receipt of the access attempt by the DB server.

16. The method of claim 15 wherein the data security decision further comprises:
selectively logging and blocking the access attempt, the data security decision including processing selected from the group consisting of firewalls, filters, intrusion detectors, alarms, alerts, tunneling and passwords.

17. The method of claim 11 wherein establishing the interface wrapper further comprises:

identifying an event corresponding to a communication via the IPC mechanism;

identifying a local event object corresponding to the event, the local event object having a notification list adapted to include registrants of an occurrence of the event; and

registering the local agent in the notification list, the local agent registered before the access gateway to receive notifications prior to receipt of the notification by the registered access gateway.

18. A method of controlling local access to a database comprising:

identifying a local access gateway to the database, the access gateway being a common access point into the database;

establishing an interception wrapper between a local client and the access gateway;

intercepting, via the interception wrapper, an access attempt from a local client prior to receipt of the access attempt by the access gateway, the access attempt indicative of a pending DB instruction in an IPC buffer

identifying a local event object corresponding to the access attempt;

indexing a notification list corresponding to the identified local event object;

traversing the indexed notification list, the notification list including entries of notifications to be performed upon occurrence of the event;

reading a traversed entry corresponding to the local agent, the entry indicative of the location of the local agent;

notifying the local agent using the read location of the local agent;

retrieving, in response to the notification, the DB instruction from the IPC buffer;

transmitting the retrieved DB instruction from the IPC buffer to a data security device operable to analyze the propriety of the DB instruction;

reading a successive traversed entry corresponding to the access gateway, the entry indicative of the location of the access gateway; and

notifying, after the notifying of the local agent, the access gateway of the IPC event occurrence using the read location of the access gateway.

19. The method of claim 18 wherein establishing the interception wrapper further comprises:

identifying, at least one interprocess communication operation, each of the identified IPC operation corresponding to an event, the event derived from a database (DB) instruction;

instantiating a local event object corresponding to the event, the local event object having a notification list indicative of notifications of an object to be made upon an occurrence of the event;

storing, in a first position in the notification list, an indication of the local agent, the first position operable to provide the first notification upon an occurrence of the event, prior to other notifications in the notification list; and

storing, in a successive position in the notification list, an indication of the access gateway, the access gateway operable to employ the IPC event for database instructions.

20. The method of claim 18 wherein the interception wrapper is operable to receive interprocess communication signaling between the local client and the access gateway, and intercepting further comprises:

receiving, by the interception wrapper, a signaling message to the access gateway;

processing the signaling message to identify an DB instruction in the register; and

passing the signaling message in a nondestructive manner to the access gateway.

21. A local agent for monitoring access to a protected database resource comprising:

a interface operable to identify an attempt to access the database resource, the access attempt being local and directed to an access gateway of the database resource;

an IPC intercept operable to intercept the identified attempt to access the database resource, intercepting occurring in a prioritized manner with respect to receipt of the access attempt by the access gateway, the local agent further operable to transmit, in a nondestructive manner, the intercepted access attempt to a local agent, the nondestructive manner operable to preserve the intercepted access attempt for successive receipt by the access gateway.

22. The agent of claim 21 wherein the access attempt is deterministic of a DB instruction, and the local agent is in communication with a data security device operable to analyze the propriety of the access attempt from objects and data values referenced by the DB instruction.

23. The agent of claim 21 wherein the local agent is operable to intercept in a prioritized manner, and further operable to:

receive the access attempt into an interception register prior to receipt by the access gateway;

invoke a prioritized request to activate a reading operation of the interception register, invoking occurring prior to activation of a read operation of the access attempt on behalf of the access gateway; and

read the access attempt from the interception register, the interception register subsequently appearing undisturbed to the access gateway.

24. The agent of claim 21 wherein the local agent is operable to, prior to identifying the access attempt, establish the IPC intercept operable to receive an IPC communication directed to the access gateway prior to receipt of the IPC communication by the access gateway.

25. The agent of claim 21 wherein the local agent is further operable to listen, at a common access point, for an incoming connection to the database resource, the common

access point adapted to aggregate access attempts to the database resource from a plurality of access mediums.

26. The agent of claim 22 wherein the local agent is further operable to reroute the intercepted access attempts to the data security device, the data security device operable to offload data security decisions as a consolidated appliance, the offloaded data security decisions relieving the host from processing the data security decisions.

27. The method of claim 21 wherein the local agent is operable to reroute local access attempts in a lightweight manner such that the data security device is operable to receive local and remote access attempts, wherein security coverage of the DB server for network and local access attempts occur via a common appliance.

28. The agent of claim 21 wherein the local agent is further operable to:

receive, from a notification object responsive to an event handler, an indication of an IPC communication indicative of a DB access attempt;

identify an instruction register in a shared memory area, the instruction register having a database instruction corresponding to the access attempt;

retrieve the DB instruction from the identified instruction register; and

transmit the retrieved DB instruction to the data security device.

29. The agent of claim 21 wherein the local agent is further operable to:

determine an IPC mechanism to be employed by a local client for accessing the DB resource;

establish an IPC intercept from a common access point employed by database clients for accessing the DB resource; and

receive the access attempt at the local agent via the IPC intercept prior to receipt of the access attempt by the access gateway.

30. The agent of claim 29 wherein the local agent is further operable to:

identify a plurality of access paths to a protected resource;

identify a common access point for the access paths to the protected resource, access attempts occurring exclusively via the identified access point for the identified access paths.

31. The agent of claim 21 wherein the local agent is further operable to:

establish an interface wrapper between the access gateway and the local client, the interface wrapper operable to identify an IPC mechanism adapted to transport communications between the access gateway and the local client; and

modify the identified IPC mechanism to inform the local agent of the communications between the access gateway and the local client prior to informing the access gateway of the communication.

32. The agent of claim 31 wherein the IPC mechanism is a shared memory portion including a plurality of instruction registers, the instruction registers operable to buffer a DB instruction for receipt by the access gateway.

33. The agent of claim 21 wherein the local agent is a lightweight agent operable to intercept the access attempt and transmit the intercepted DB instruction to a data security device, the local agent having a substantially insignificant effect on a DB host supporting the DB server.

34. The agent of claim 21 wherein the local agent is further operable to:

block the intercepted access attempt from receipt by the access gateway, and

selectively unblock the access attempt depending on a data security decision.

35. The agent of claim 34 wherein the local agent is responsive to the data security device for:

computing the data security decision at the data security device; and

transmitting the data security decision to the local agent, the local agent operable to permit receipt of the access attempt by the DB server.

36. The agent of claim 35 wherein the data security device is operable to selectively log and block the access attempt, the data security decision including processing selected from the group consisting of firewalls, filters, intrusion detectors, alarms, alerts, tunneling and passwords.

37. The agent of claim 24 wherein the local agent is further operable to:

identify an event corresponding to the communication via an IPC mechanism;

identify a local event object corresponding to the event, the local event object; having a notification list adapted to include registrants of an occurrence of the event; and

register the local agent in the notification list, the local agent registered before the access gateway to receive notifications prior to receipt of the notification by the registered access gateway.

38. A data security device for monitoring access to a protected database resource comprising:

a memory;

a processor operable to execute instructions in the memory;

an interface operable for interconnection with a database host, the data security device in communication with a local agent on the database host, the local agent operable to:

identify an attempt to access the database resource, the access attempt being local and directed to an access gateway of the database resource;

intercept the identified attempt to access the database resource, intercepting occurring in a prioritized manner with respect to receipt of the access attempt by the access gateway; and

transmit, in a nondestructive manner, the intercepted access attempt to a local agent, the nondestructive manner operable to preserve the intercepted access attempt for successive receipt by the access gateway.

39. A computer program product having a computer readable medium operable to store computer program logic embodied in computer program code encoded thereon for monitoring access to a protected database resource comprising:

computer program code for identifying an attempt to access the database resource, the access attempt being local and directed to an access gateway of the database resource;

computer program code for intercepting the identified attempt to access the database resource, intercepting occurring in a prioritized manner with respect to receipt of the access attempt by the access gateway; and

computer program code for transmitting, in a nondestructive manner, the intercepted access attempt to a local agent, the nondestructive manner operable to preserve the intercepted access attempt for successive receipt by the access gateway.

40. A computer data signal having program code for monitoring access to a protected database resource comprising:

program code for identifying an attempt to access the database resource, the access attempt being local and directed to an access gateway of the database resource;

program code for intercepting the identified attempt to access the database resource, intercepting occurring in a prioritized manner with respect to receipt of the access attempt by the access gateway; and

program code for transmitting, in a nondestructive manner, the intercepted access attempt to a local agent, the nondestructive manner operable to preserve the intercepted access attempt for successive receipt by the access gateway.

41. A security filter device for behavior based access tracking of a software application comprising:

means for identifying an attempt to access the database resource, the access attempt being local and directed to an access gateway of the database resource;

means for intercepting the identified attempt to access the database resource, intercepting occurring in a prioritized manner with respect to receipt of the access attempt by the access gateway; and

means for transmitting, in a nondestructive manner, the intercepted access attempt to a local agent, the nondestructive manner operable to preserve the intercepted access attempt for successive receipt by the access gateway.

5